DOMINIK ROBAKOWSKI

MAŁA KSIĘGA WIELKICH SZYFRÓW

Helion
EDUKACJA

Redaktor prowadzący: Małgorzata Kulik

Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/malksi
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-0193-3

Printed in Poland.

Spis treści

Pierwsze urządzenia szyfrujące

Szyfr Albertiego

Choć poznaliśmy już najbardziej skomplikowane szyfry tworzone bez ingerencji maszyn, to jednak trzeba uznać, że mimo swojej pomysłowości miały one dość znaczącą wadę. Z oczywistych względów nie były odporne na błędy, których dopuszczał się czynnik ludzki. Rozwój komunikacji (telegraf, a później radio czy wreszcie internet) sprawi, że w pewnym momencie dziejów (pierwsza połowa XX wieku) szyfry kreślone ludzką ręką stracą na znaczeniu na rzecz rozwiązań generowanych przez maszyny. Ten obszerny i osobny rozdział kryptologii ma swoich nieśmiałych protoplastów. Poznajmy proste urządzenia, które pomagały w szyfrowaniu wiadomości.

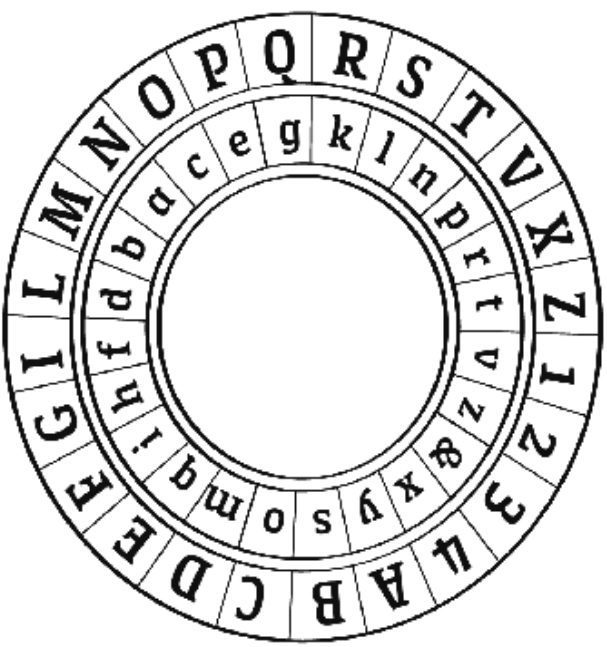
Pierwszym, choć jak już wiemy, niezwykle prymitywnym urządzeniem służącym do szyfrowania były greckie skytale. Poważniejsze prace nad „maszyną" szyfrującą pojawiły się dopiero w okresie renesansu. W XV wieku na kryptologicznej scenie wyróżnił się Leon Alberti i jego słynne dyski.

Wynalazek ten okazał się niezwykły nie tylko dlatego, że ułatwiał proces szyfrowania, ale też z tego powodu, że był jedną z pierwszych prób budowania szyfrów polialfabetycznych. Przyjrzyjmy się urządzeniu Albertiego (alfabet odpowiada używanemu wówczas alfabetowi włoskiemu).

Mechanizm, o ile możemy o nim tak mówić w wypadku do tego stopnia prostego urządzenia, składał się z dwóch dysków zamontowanych

na wspólnej osi. Szerszy dysk (zwany przez Albertiego nieruchomym) zawierał duże litery w kolejności alfabetycznej, odpowiadały one tekstowi jawnemu. Dysk wewnętrzny (ruchomy) posiadał małe litery w losowej kolejności, które stanowiły alfabet szyfrujący. Ważne było, aby nadawca i odbiorca posiadali identyczny komplet dysków. Dodatkowo obie strony ustalały tzw. wskaźnik, czyli początek alfabetu szyfrującego — w naszym wypadku będzie to litera a.

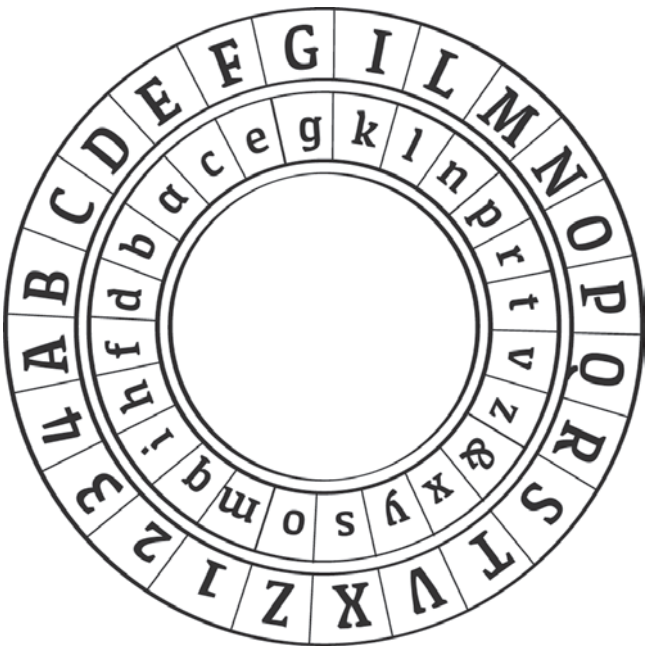
W przykładzie będziemy chcieli zaszyfrować imię i nazwisko twórcy — LEON ALBERTI. Skorzystajmy z ustawienia dysków widocznego na ilustracji poniżej. Zasygnalizujmy jego wygląd odbiorcy wiadomości. W tym celu odnajdźmy nasz wskaźnik (literę a na wewnętrznym dysku). Literę, która znajduje się nad nim (czyli N), zapiszmy do szyfrogramu na samym początku — od tej pory odbiorca wie, jak ustawić swoje urządzenie.



Zaszyfrujmy pierwsze słowo — zamieniamy litery jawne z zewnętrznego dysku na odpowiedniki z dysku wewnętrznego:

LEON → N dica

Alberti wpadł na pomysł, aby co jakiś czas zmieniać ułożenie dysków względem siebie. Pozwalało to na użycie nowego alfabetu szyfrującego. Na poniższym rysunku widać modyfikację. Nasz wskaźnik (a) znajduje się teraz pod literą D. Sygnalizujemy to zajście w szyfrogramie umieszczeniem w nim dużej litery D. Następnie kolejne słowo szyfrujemy już zgodnie z obecnym ustawieniem dysków:



ALBERTI → D fldczxk

Ostatecznie nasz szyfrogram uzyska postać NdicaDfldczxk.

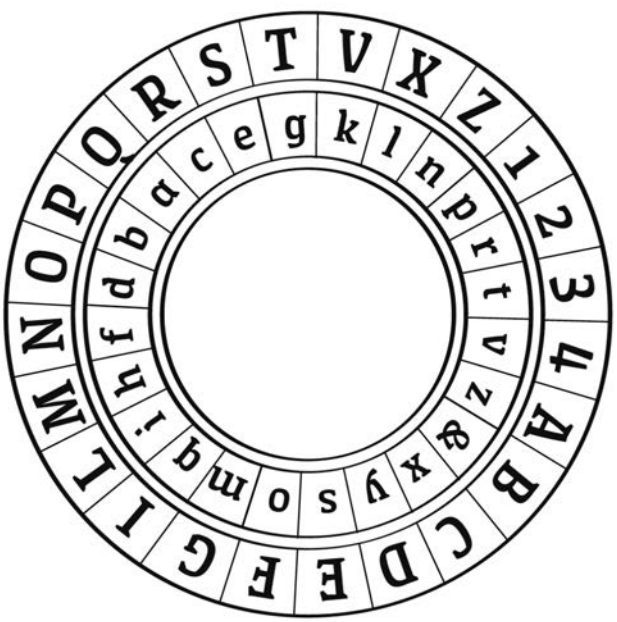
Odbiorca wiadomości odtwarzał proces szyfrowania za pomocą swojego dysku. Najpierw ustawiał wskaźnik zgodnie z sugestią szyfrogramu (N nad a). Następnie odszukiwał w szyfrogramie poszczególne litery

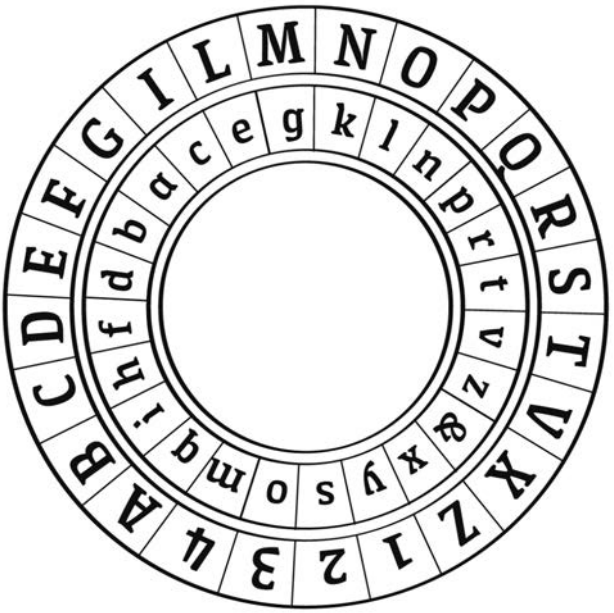
z dysku wewnętrznego i przekładał je na te, które znajdowały się na dysku zewnętrznym. W momencie zauważenia kolejnej litery (D) przekręcał dysk tak, aby znajdowała się ona nad wskaźnikiem (D nad a).

Dysk Albertiego jest jednym z najważniejszych wynalazków w dziejach kryptologii. Złamanie szyfrogramu bez przejęcia dysków było praktycznie niemożliwe. Oczywiście istnieje cały szereg modyfikacji, które sprawiają, że urządzenie jest jeszcze bardziej bezpieczne i wygodne w użytkowaniu. Jedna z wersji wynalazku Albertiego używana była jeszcze w czasie wojny secesyjnej. Dla utrudnienia zamiast liter szyfrogramu występowały w niej kody liczbowe.

Zadania

1. Zaszyfruj frazę OBCA ARMIA, korzystając z poniższego dysku. Pierwszy wyraz zaszyfruj przy pierwszym ustawieniu urządzenia, drugi przy drugim. Pamiętaj o umieszczeniu informacji o pozycji dysków względem siebie (wskaźnikiem tym razem jest litera e).



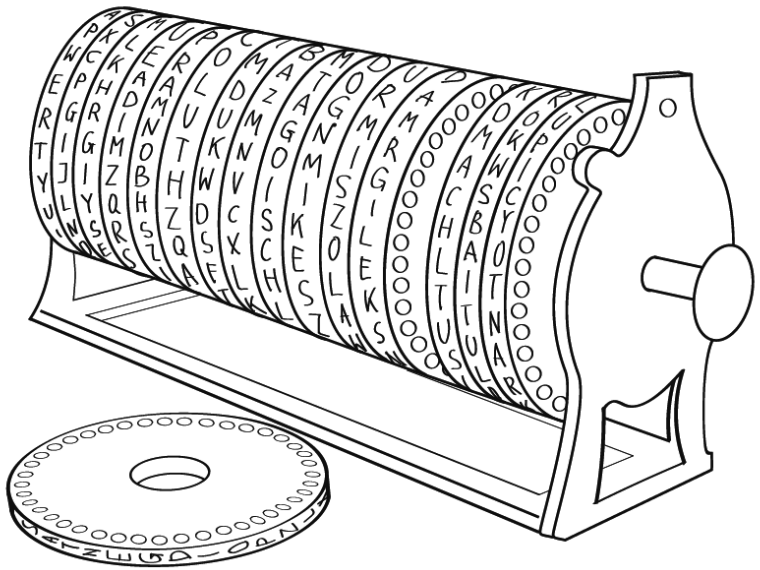


2. Zbuduj własny dysk Albertiego — wystarczą Ci kartka, ołówek, nożyczki i pinezka, która wyznaczy wspólną oś. Oczywiście możesz zastosować współczesny alfabet.

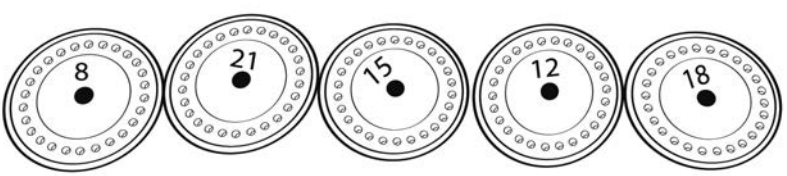
Szyfr Jeffersona

Prezydenci Stanów Zjednoczonych zrzucają bomby atomowe, występują w westernach, grają na saksofonie. Chyba nikt nie będzie więc zdziwiony, że jednemu z nich udało się wymyślić bardzo ciekawą maszynę szyfrującą.

Mowa tutaj o Thomasie Jeffersonie. Swój wynalazek stworzył on jeszcze przed objęciem urzędu. Nasz bohater zbudował prosty mechanizm, nazywany cylindrem, złożony z kilkudziesięciu krążków umieszczonych na wspólnej, łatwej do wyjęcia osi. Każdy z krążków posiadał na sobie 26-literowy alfabet o niepowtarzalnym układzie liter. Poza tym każdy dysk posiadał swój numer.

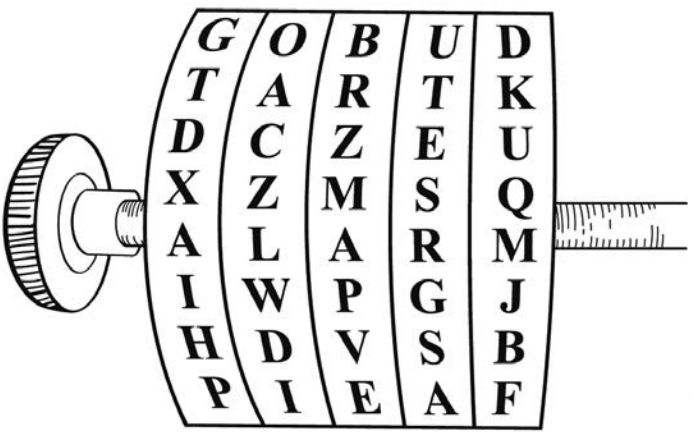


Szyfrant rozpoczynał swoją pracę od przygotowania „maszyny" zgodnie z obowiązującą w danym dniu procedurą. W praktyce oznaczało to ułożenie dysków zgodnie z poleceniem oficera. Jeśli w danym dniu zakładano, że pierwsza litera szyfrogramu będzie szyfrowana dyskiem nr 7, druga — nr 20, a trzecia — nr 13, to w takiej kolejności szyfrant „nadziewał" je na oś. Oczywiście odbiorca wiadomości przygotowywał swoje urządzenie w podobny sposób.



Teraz, przesuwając dyski względem siebie, szyfrant układał tekst jawny. Aby przypadkiem elementy nie ulegały przesunięciu, stabilizowano je za pomocą metalowej szpili, którą przewlekano przez jeden z 26 otworów znajdujących się w dysku.

Kolejnym krokiem było przepisanie jednej z 25 linii, które powstały powyżej lub poniżej tekstu jawnego. To już gotowy szyfrogram, który możemy nadać do odbiorcy.



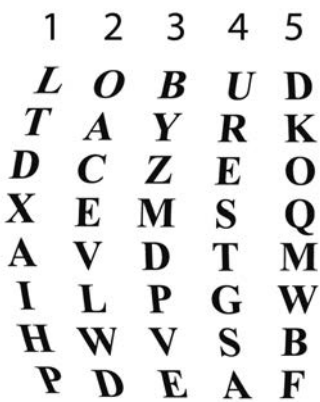
Jak wyglądał odczyt? Zadaniem odbiorcy było ułożenie dysków w tej samej kolejności oraz ułożenie szyfrogramu. Teraz wystarczyło już tylko przejrzeć 25 powstałych linii, aby odnaleźć wśród nich tekst jawny.

Szyfr ten w swoim czasie uchodził za dość bezpieczny. Istniały jednak pewne niedogodności. Proces szyfrowania był długotrwały, a ilość ukrywanego tekstu była stosunkowo nieduża. Produkcja dysków też nastręczała pewnych problemów, pomijając, że zawsze istniało ryzyko, że gotowe urządzenie wpadnie w ręce wroga — poznanie alfabetów szyfrowych wymagało zmian w całej sieci łączności. Co ciekawe, szyfru Jeffersona w zmodyfikowanej formie używano jednak jeszcze w czasie drugiej wojny światowej, choć dla poślednich zadań.

Zadania

1. Fizyczny brak dysków Jeffersona sprawia, że musisz poćwiczyć wyobraźnię. Poniżej zaprezentowano pięć dysków, które posłużą nam do odczytania nadanego szyfrogramu. Spróbuj ułożyć je w odpowiedniej kolejności, połączyć poszczególne litery szyfrogramu ze sobą oraz odszukać hasło.

Ustawienie dysków: 3 4 1 5 2
Szyfrogram: ZSHFC



Szyfr paskowy

Można tworzyć skomplikowane i piękne urządzenia? Można. Zawsze jednak przegrają one ze swoimi budżetowymi odpowiednikami.

Szyfr paskowy stanowił tańszą wersję pomysłu Jeffersona. Zamiast odlewni metalu wystarczą nam nożyczki i karta papieru. Jakby nie patrzeć — wychodzi taniej.

Zobaczmy, że aby uzyskać efekt podobny do cylindra Jeffersona, możemy po prostu „rozwinąć" dyski, tworząc kilkanaście pasków zawierających 26 różnych alfabetów. Aby praca była wygodniejsza i imitowała zachowanie dysku, każdy z alfabetów na pasku dublowano. Spójrzmy

na nasz uproszczony przykład, w którym wykorzystamy jedynie pięć krótkich pasków.

A B C D E F G H I J K L M N O P Q R
X Y B A C G I L O T N R S T U V W D
H S T Q W X Y A O P E N B V C Z K L
P O I U Y T R E W Q A S D F G H J K
T G B M J U Y H N K I O L P C D Q A

Musimy teraz ustalić kolejność ułożenia pasków, podobnie jak czyniono to z dyskami szyfru Jeffersona. Można było zrobić to, przypisując poszczególnym szyfrom cyfry lub wymyślając słowo klucz, które odpowiadałoby pierwszym literom poszczególnych alfabetów. W naszym wypadku klucz będzie brzmiał PATHX — w tej kolejności układamy paski:

P O I U Y T R E W Q A S D F G H J K
A B C D E F G H I J K L M N O P Q R
T G B M J U Y H N K I O L P C D Q A
H S T Q W X Y A O P E N B V C Z K L
X Y B A C G I L O T N R S T U V W D

Teraz nadszedł czas, aby ułożyć tekst jawny poprzez przesuwanie względem siebie poszczególnych pasków w lewo lub prawo. Aby ułatwić sobie pracę, wiadomość umieszczano w specjalnej ramce. Po wykonaniu tego procesu szyfr powinien przypominać krzyżówkę, której „hasłem" jest tekst jawny.

P **O** I U Y T R E W Q A S D F G H J K
A B C D E F G H I J **K** L M N O P Q R
T G B M J U Y H N K I **O** L P C D Q A
H S T Q W X Y A O **P** E N B V C Z K L
X **Y** B A C G I L O T N R S T U V W D

Dobrze, gdzie więc znajduje się nasz szyfrogram? Podobnie jak w wypadku dysków Jeffersona będzie nim układ sąsiadujący z tekstem jawnym. Ponieważ ze względów technicznych nie ma tym razem możliwości wybrania dowolnego szyfrogramu (pracujemy na „rozwiniętych" dyskach), szyfranci najczęściej umawiają się na stałą wartość przesunięcia. W naszym przypadku niech będą to dwie pozycje w prawo od tekstu jawnego.

P **O** I **U** Y T R E W Q A S D F G H J K
A B C D E F G H I J **K** L **M** N O P Q R
T G B M J U Y H N K I **O** L **P** C D Q A
H S T Q W X Y A O **P** E **N** B V C Z K L
X **Y** B **A** C G I L O T N R S T U V W D

Tak przygotowany szyfrogram bez problemu mógł zostać odebrany w innym miejscu. Wystarczyło odtworzyć kolejność alfabetów i odnaleźć szyfrogram. Pozostawało jeszcze namierzyć tekst jawny, przesuwając się tym razem o dwie pozycje w lewo.

Żywotność tego systemu była dość długa. Różne wariacje na jego temat funkcjonowały jeszcze w czasie zimnej wojny. Ot, czasem szpieg musi działać bez prądu.

Zadania

1. Poniższy szyfr ma już właściwą kolejność pasków oraz ułożony szyfrogram. Czy jesteś w stanie odnaleźć tekst jawny?

H S T Q W X Y A O P E N B V C Z K L
D E F G H I J K L N O P Q R A B C
T G B M J U Y H O K I G L P C D Q A
X Y B A C I G L O T N R S T U V W D
P O T U Y I R E W Q A S D F G H J K

2. Spróbujmy czegoś trudniejszego. Poniżej znajdują się przykładowe paski, które pomogą Ci odkryć kolejne hasło. Przepisz je na kartkę w następującej kolejności: HDPXB. Zrób to tak, aby powstał szyfrogram QHULM. Cztery pozycje na prawo od niego odnajdziesz hasło.

D E F G H I J K L N O P Q R A B C
X Y B A C I G L O T N R S T U V W D
P O T U Y I R E W Q A S D F G H J K F G H J K
H S T Q W X Y A O P E N B V C Z K L
B G H M J U Y T O K I G L P C D Q A

3. Być może poprzednie zadanie wydaje Ci się dość żmudne i być może zdarzyło Ci się dokonać kilku nieestetycznych skreśleń. Spróbuj rozwiązać szyfrogram jeszcze raz, ale tym razem stwórz prawdziwe paski (z takim samym układem liter jak w ostatnim zadaniu), które będziesz mógł wyciąć, a potem przesuwać względem siebie. Nasz klucz to tym razem XPBDH, natomiast szyfrogram to YYGGX. Dwie pozycje na prawo od niego znajdziesz rozwiązanie zadania.

Choć pierwsze maszyny szyfrujące zdają się być dość prymitywne, to jednak znacząco ułatwiały pracę kryptologów. Prawdziwy przełom nastąpił jednak dopiero w XX wieku, gdy w kilku niezależnych od siebie ośrodkach opracowano maszyny wirnikowe, mogące w prosty sposób budować niezwykle skomplikowane szyfry. Klasyczna kryptologia nadal jednak odgrywała swoją rolę. Kres jej popularności położyły dopiero szyfry generowane przez komputery. To już jednak temat na zupełnie inną opowieść…


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

KRYPTOLOGIA JEST TRUDNA? MOŻE, ALE NA PEWNO NIE Z TĄ KSIĄŻKĄ!

Jeśli słowo „szyfr" budzi w Tobie przyjemny dreszczyk emocji, mamy dla Ciebie prawdziwą gratkę. Już za chwilę poznasz największe tajemnice ludzkości. Prezentowane w tej książce tajemnicze kody służyły dyplomatom, armiom pierwszej i drugiej wojny światowej, wreszcie zimnowojennym szpiegom. Były kamyczkami, które wywołały lawinę rewolucji informatycznej. Bez żadnej przesady — oto szyfry, które decydowały o losach świata. I wciąż o nich decydują.

Kryptologia bardzo intensywnie się rozwija. Dziś jest wręcz niezbędna do naszego funkcjonowania. Warto poznać jej podstawy, tak samo jak wypada się orientować w historii, fizyce czy biologii — choćby po to, by być na bieżąco ze współczesną nauką. Poza tym szyfrowanie i deszyfrowanie stanowi znakomitą gimnastykę dla umysłu i dobry sposób na kreatywne spędzenie czasu. Co więcej, prezentowane sposoby ukrywania wiadomości mogą nadal służyć zgodnie ze swoim pierwotnym przeznaczeniem — do ukrywania tego, co niekoniecznie chcemy przekazać wprost...

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-289-0193-3

Cena: 39,00 zł